User Controlled Privacy in Participatory Sensing

Ramaprasada R. Kalidindi, KVSVN Raju[1], V. Valli Kumari[2], C.S. Reddy[3]
Dept. of Computer Science and Engineering,
S.R.K.R. Engineering College,
Bhimavaram-534204, India.
rrkalidindi@computer.org
Dept. of Computer Science and Systems Engineering,
AUCE(A), Andhra University,
Visakhapatnam-533003, India.
[1]kvsvn.raju@gmail.com, [2]vallikumari@ieee.org, [3]csatyanand@gmail.com

***Abstract*—Most of the sensor network applications in military and civilian use are surreptitious. If these are used for the benefit of society in addition to the individual needs a new set of applications can be developed. This paper describes infrastructure monitoring based on collaboration between sensor networks. The solution provides a reputation based hybrid network where collaborative trust is established based on referrals (opinions). Depending on the trust, the information is exchanged between one entity and another with different authorization levels. The outcome of the paper is collaborative data collection with privacy levels controlled by individual users.**

***Keywords*- privacy control; trust; reputation; collaborative networks; urban sensing; participatory sensing; sensor networks.**

I. INTRODUCTION

Widespread use of low cost tiny sensors in civilian applications and their eventual integration with Internet has made them pervasive [1, 2, 3]. Often data collected from sensor networks in the urban environments inhabited by humans constitute personal information. The acceptance of these sensor networks as public infrastructure will need citizens' participation and collaboration. This type of applications in urban areas is entirely different from habitat monitoring, where privacy is not a concern. Deploying these networks without addressing the security and privacy concerns will turn against those whom it is meant to benefit. And user acceptance depends on the provision of appropriate mechanisms to deal with these concerns. The main privacy problem in sensor networks is; they generate large volumes of information which is easily available through remote access. Ensuring that sensed information stays within sensor network and is accessible only to trusted parties is an essential step toward achieving privacy [4].

Allowing individual's control on how personal data is collected, distributed and processed addresses privacy (information privacy) issues. This can be achieved by providing a resolution control in the hands of the user. High resolution data is more useful, but this choice could be left to the individual provider so that privacy control can be done at the source [5, 6]. In an urban environment establishing a sensor network over large area is not practically feasible due to cost, but with people's participation this can be done with minimum cost. For example, consider these two applications.

First, the civic authorities in metropolitan cities provide general amenities and security to public depending on the time variant density of population during work hours in offices, evening at parks, and night at clubs etc. This may vary during week days, weekends, festivals, functions and meetings. Estimating the requirement and deploying the security personnel and ambulances and other amenities dynamically is not precise, as getting the real time data is difficult and costly. Assuming that each person has a cell phone, the population density of people at a point of time can be identified using cell phone location [7].

Second, the spread of a contagious disease and its consequences are known to public and health authorities only after certain causalities. But estimating the disease spread in real time depending on the people queries to health websites (*viz* Google flu trends) minimizes causalities and certain areas can be quarantined in advance [8]. Sharing person specific data for this type of applications is not possible without the consent of its owner. If the granularity of the data is high, there will be more applications of this kind.

Automatic collection of higher granular data is possible with networked sensors at higher densities. When these are used around human habitats they will collect human related data, but people do not want to make private life public. Most of the today's sensor network applications are pervasive in nature in which a centralized authority is used to collect data from individuals. But the individuals are not having any control over their private data. For example, giving cell phone location to unauthorized agencies is not allowed under privacy laws. If an individual is willing, this information can be shared with others. People may not be willing to share this information at all times. If the individual is having control over when to share and what to share, more people will allow sharing. This will lead to new applications like location advertising, alerting nearest emergency services etc., where collaborative and opportunistic sensing is used to realize pervasive applications [9]. More people will participate in these endeavors if privacy control is with individual rather than with centralized authority.

DOI: 01.IJNS.01.03.187

For infrastructure monitoring applications in gated communities, apartment buildings and rented commercial complexes, solutions are provided with different networks for different tasks like power management, water management, security and surveillance etc. With the availability of sensors with multi-sensing capabilities and Internet connectivity, these independent networks can be converted to a single IP based Building Information Network [10] to reduce the overall cost. This development in sensor networks will reduce man power and other costs for the infrastructure developer and facilitate monitoring of the property remotely by the owners. If the owner is willing, these networks can be integrated to have pre-installed sensor networks by the developer. The owner will not accept developer control over his/her private data. If solutions are available to have control with the owner, he/she may be interested to share some data willingly. Each owner can establish or can accept pre-installed individual network and it can be integrated with other individual sensor networks to form an integrated network and maintained by a third party. These sensor networks maintained at a residential locality can be integrated with another network through Internet. This will create an urban infrastructure for solid waste management, pollution control, disaster management, etc., for the benefit of citizens.

To this end, we described a model for infrastructure monitoring by collecting data from individual wireless sensor networks (WSNs). The rest of the paper is organized as follows: Section II describes related work, section III describes collaboration based information monitoring, section IV contains description of the model and the trust value representation and assumptions, section V provide the evaluation of the model and section VI concludes the paper and suggests possible future directions.

II. Related Work

Giang et al. [11] proposed a scheme to control privacy exposure by trust evaluation on the basis of previous transactions and peer recommendation. The authors developed a methodology to estimate trust value and depending on this trust, users can have a privacy policy to decide about how much data can be given to others. The solution is for sharing personal data in the computer in a ubiquitous environment.

The hybrid trust management scheme by Shaik et al. [12] minimizes resource utilization at sensor nodes with a hierarchical distributed WSN, where the group has a trust value. The authors presented a trust model which calculates trust in three phases at node, cluster head and base station.

Chen et al. [13] presented a scheme for trust rating propagation by on demand and trigger methods in WSNs. The authors aggregated the trust rating from other nodes with node's trust value from its own observation.

Mitseva et al. [14] presented a privacy protection mechanism with context aware trust establishment for applications in medical and vehicular network scenarios. The authors integrated this mechanism into the hybrid hierarchical WSN using anonymization and controlled information disclosure.

III. Collaboration Based Infrastructure Monitoring

A. Application Scenario

Monitoring the flats in apartment buildings, houses in gated communities and shops in commercial complexes use video surveillance networks for maintaining security and other sensor networks for maintenance by the developer. The owners of the flats (or houses/shops) can also have their own sensor networks to monitor their property. The model describes sensor networks in apartment buildings, but it can also be applied to the other applications above.

B. Network Model

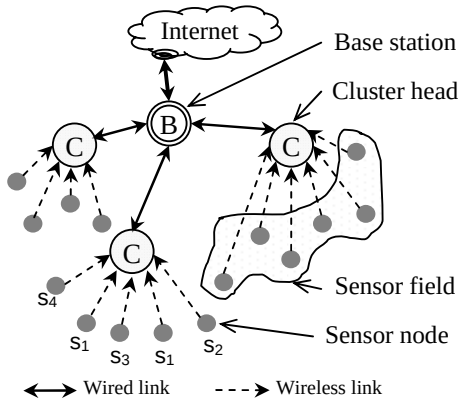


Figure 1 Hierarchical Wireless Sensor Network

The proposed model in Fig. 1 is a hierarchical architecture for integration of sensor networks with Internet.

Wireless sensors ease the deployment[1]. The sensors deployed in a flat (sensor field) are connected to a station called *Cluster Head* (C) stationed in each flat. Each *Sensor Node* sends data to cluster head. The cluster head stores data from all sensors, so that the owner of the flat can decide with whom he/she can share the data. If the flat was rented, the owner can delete private data from the cluster head and after that the tenant will be the owner of the data. These cluster heads are connected to a *Base Station* (B) maintained by maintenance authority and in turn the base station is connected to Internet. The cluster head will share certain infrastructure related data like overhead water tank level etc. with the base station. The base station will

[1] The sensor nodes are installed through a cluster head and the security key is only known to the particular cluster head. Since the wireless signal can be received by any cluster head within the range, the data is encrypted and only the corresponding cluster head can decrypt. Unidirectional wireless links shown in Fig. 1 are secure links connected to cluster head.

DOI: 01.IJNS.01.03.187

maintain shared data and participate in urban infrastructure through Internet.

The data collection mechanism is composed of four levels viz. sensor node, cluster head, base station and emergency agencies through Internet. Sensor nodes collect data from physical activity and send it to cluster head. The cluster head updates data at the base station periodically. Emergency management agencies can access data at base station through Internet to deal with emergencies or the base station can alert the agency in case of emergencies. Authorized users can access data at the cluster heads and base station. This work attempted to give access to data among trusted parties by finding the trustworthiness using reputation.

Sensor Nodes (s_1-s_4) collect data about the physical activity like state of bedroom door, light, overhead water tank level, fire alarm etc. They transmit this data to Cluster Head (C). The cluster heads are connected to Base Station (B). The base station sends emergency data to emergency services which are connected through Internet. The links between sensor nodes and cluster head are unidirectional. The link between cluster head and base station is bidirectional. These links are secured and the base station is connected to Internet.

This model assumes a multi-owner and multi-user network with sensor nodes, which continuously produce data. The owners of different cluster heads can categorize sensors as s_1 to s_4. Table I gives the type of data from various sensors.

TABLE I
TYPES OF SENSORS

Sensor	Data of interest
s_1	State of bed room door, light, etc. (Personal)
s_2	State of living room door, water heater, A/C etc. (Flat utilities)
s_3	Overhead tank water level, power meter reading, etc. (Maintenance utilities)
s_4	Fire, theft alarm, earth quake detection, etc. (Emergency)

The owners of cluster heads, administrator at base station and disaster management teams which are using the emergency sensors' data will be the users of network. At each cluster head, there are four authorization levels A_1 to A_4 to access different types of data. Table II gives the authorization levels. These levels will determine to what extent the user can have access to data.

TABLE II
USER AUTHORIZATION LEVELS

Level	Users
A_1	Self
A_2	Trusted friends
A_3	Infrastructure maintenance authority
A_4	Emergency services (Fire services, police, disaster management teams, etc.)

A user authorized at level A_1 can have access to entire data at cluster head level, has privileges to give authorization for other users and can configure the sensor network. At level A_2 data from sensors s_2, s_3 and s_4 can be accessed. At level A_3 data from s_3 and s_4 sensors can be accessed. At level A_4 data from s_4 sensors can be accessed. The data from s_4 sensors is generated in emergencies and is available through base station. Since the owner of information can authorize others for different levels of authorization, the access control will be with owner. All cluster heads send data from s_3 and s_4 sensors to base station. The data from s_1 sensors is personal and is accessible to the owner only. The data from sensors s_2, s_3 and s_4 can be shared with neighbors. They can access this data at their cluster head through a secured link provided by base station, since each cluster head is connected to base station.

The authorization level A_2, assigned to different cluster heads may be withdrawn if the occupant of a flat does not have the trust on them. In a social community, trust between two individuals is developed based on their transactions over time. When a flat owner who is in control of cluster head wants to share information with friendly neighbors, he/she can trust only few neighbors. When these neighbors are changing continuously (new owners and new tenants) trusted neighbors are to be identified dynamically. For example, if the owner of a flat gives it for rent, the sensor network collects tenant's data. The tenant may not be interested in sharing his/her data with owner's trusted friends, who may not be his/her trusted friends. This requires calculation of trust about other cluster heads at the cluster head periodically. When faced with uncertainty, individuals trust and rely on the previous transactions and opinions of others who have good transactions with them in the past.

Initially when a new owner approaches maintenance authority for a flat, they will undertake an agreement which is a legally binding document on two parties. This document will give an initial trust, which is called as *institutional trust*, between them. An owner develops a reputation for each other owner by making direct observations about other owners in the neighborhood. This reputation is used to help an owner evaluate the trustworthiness of others and make a decision to share data within the network.

IV. PROPOSED MODEL

In social environment, we trust people depending on past interactions with them. These past interactions will be used to build reputation of a particular person. In the absence of these interactions, we take the opinion of others to build initial trust. In the network model described in Section III.B, the data is stored with the cluster head and it is exchanged with base station and other cluster heads, depending upon their authorization levels. We have to trust the entities behind these cluster heads and authorization levels are to be entrusted to each entity. Since this trust is

DOI: 01.IJNS.01.03.187

needed in between the entities which are dealing with authorization, only the network of base station and cluster heads is considered. The terminology used in the remaining sections is given below.

Base station (B) is the maintenance authority, which will maintain data coming from the cluster heads pertaining to certain sensors and is connected to all cluster heads and the Internet.

Node (N) is the cluster head which will collect data from sensor nodes and forward certain type of sensors' data to the base station.

Neighbor is one of the remaining cluster heads which is connected to base station with which a cluster head wants to share information or collect opinion.

Opinion (O_{xy}) is the value given by a node *x* depending upon the reputation of *y*.

A. Reputation

Reputation of a node is the satisfaction of usage of shared data and its reciprocation in sharing data. As part of infrastructure, the nodes are sharing part of the data with base station. The base station gives reputation ratings depending on their participation in sharing the data. A node can also share data with another node and it gives reputation rating depending on how the other node is using the shared data and whether it is sharing data with it or not. A node can take reputations from other nodes and can derive an opinion value considering the reputations and its own transactions.

Let there are *n* nodes (N_1 - N_n) connected to base station, B. The *Reputation* of a neighbor N_j at node N_i is derived from direct reputation of N_j at N_i and observed reputation of N_j collected from other nodes and base station at N_i. The *direct reputation,* R_{ij}^e is an event driven reputation of a node N_j as perceived by node N_i when it is directly transacting with node N_j and $R_{ij}^e \in [0,1]$. The *observed reputation* R_{ij}^o of a node N_j as perceived by node N_i reflects the N_j's behavior with neighbors in the community and $R_{ij}^o \in [0,1]$. The base station is having transactions with all other nodes. The nodes may or may not have transactions with other nodes; t_{ij} is the total and t_{ij}^s is the successful number of transactions between nodes N_i and N_j.

The base station and each node will maintain a reputation table consisting of direct reputation of the node and total number of transactions with that node for base station and all nodes in the network. The self reputation value is one (i.e., $R_{ii}^e = 1$). All transactions to itself are successful transactions (i.e., $t_{ii} = t_{ii}^s$).

Fig.2 shows transactions between base station and nodes. Thick line indicates transaction and dashed line indicates a request to get opinion.

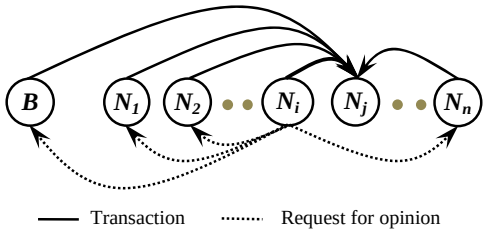


Figure 2. Interactions with nodes to obtain N_j's reputation

When a node N_i wants to calculate the trust of a particular node N_j it sends a broadcast request to base station and all other nodes. These nodes will respond to this request by sending the reputation of N_j, and the total number of transactions with N_j, which are available in their respective reputation tables. Responding to the request is treated as positive transaction which will increase the reputation of responding node there by encouraging responses. Every time a node interacts with other node it updates its reputation table.

B. Direct Reputation

The *direct reputation* R_{ij}^e is the ratio of successful and total transactions of node N_i with node N_j. When a node requests for information from a node, if other node responds by sending the information it will be treated as successful transaction; no response will be treated as unsuccessful transaction. When a node N_i is having t_{ij} total transactions and among them t_{ij}^s is the successful number of transactions with N_j, the direct reputation is given as in (1).

$$R_{ij}^e = \frac{t_{ij}^s}{t_{ij}} \qquad (1)$$

In a social environment, when we deal with persons, we form an opinion taking the reputation of that person in the community into account. It may be a positive or negative opinion depending on various inputs we have about that person. The definition of *opinion,* as given by Oxford dictionary, is a belief or judgment about a particular thing, which is not necessarily based on fact or knowledge. If reputation is considered to form an opinion, more than half of successful transactions be considered as positive and less than half be as negative. The personal opinion O_{ij}^p of node N_i about N_j is given as in (2).

DOI: 01.IJNS.01.03.187

$$O_{ij}^{p} = \begin{cases} \left(R_{ij}^{e} - 0.5\right) & if \quad t_{ij} \neq 0 \\ 0 & if \quad t_{ij} = 0 \end{cases} \qquad (2)$$

$O_{ij}^{p} \in [-0.5, 0.5]$, *a* positive value represents positive opinion and negative value represents negative opinion.

C. Observed Reputation

The *observed reputation* R_{bj}^{o} is derived from the reputation collected from base station by node N_i about N_j and base station reputation at node N_i. For example, if N_i requests base station to send data about N_j, the base station sends R_{bj}^{e} and t_{bj} values. The reputation R_{ij}^{o} is derived from the direct reputation value R_{bj}^{e} received from base station and direct reputation R_{ib}^{e} stored at node N_i about base station as in (3).

$$R_{bj}^{o} = R_{ib}^{e} \cdot R_{b\,j}^{e} \qquad (3)$$

Opinion (o_{bj}) of base station about node N_j is given as in (4).

$$o_{bj} = \begin{cases} \left(R_{bj}^{o} - 0.5\right) & if \quad t_{bj} \neq 0 \\ 0 & if \quad t_{bj} = 0 \end{cases} \qquad (4)$$

$o_{bj} \in [-0.5, 0.5]$, since the opinions collected from base station and other nodes may not match with each other, these are rounded to one decimal place so that majority opinion is selected. Let $S = \left(o_{bj}, o_{1j}, o_{2j}, \ldots\ldots o_{nj}\right)$ be the set of opinions (rounded to one decimal place) from base station and other nodes. The majority of the observed opinions O_{ij}^{o} is given as $O_{ij}^{o} = M(S)$, where M is a function to find the mode of given set of opinions S from base station and other nodes.

D. Evaluating the Opinion

The overall opinion O_{ij} is node N_i's opinion on N_j and is given as in (5).

$$O_{ij} = w_i O_{ij}^{p} + (1 - w_i) O_{ij}^{o} \qquad (5)$$

Where w_i is the weight assigned to personal opinion among personal and other's opinion at N_i. When a node is having sufficient number of transactions to judge, there is no necessity of taking other's opinions. If a node is having total transactions more than the average total transactions done by other nodes, the node will take only its opinion into account ($w_i = 1$) otherwise other's opinion is also considered then the weight w_i is given as in (6).

$$w_i = \frac{nt_{ij}}{\sum_{k=b,1}^{n} t_{kj}} \quad \text{if} \quad t_{ij} < \frac{\sum_{k=b,1}^{n} t_{kj}}{n} \qquad (6)$$

Users at cluster heads collect opinions and consider them in establishing trust with neighbors. Depending on this trust they authorize users to different levels, thereby having the control to which they have to share their data.

V. Model Evaluation

In the housing infrastructure having hundreds of houses at particular place is quite common, but having thousands of houses in a single project is very rare. For evaluating our model we have taken one hundred nodes having trasactions upto ten thousand. Opinions were derived from the reputations and majority opinion is taken for consideratrion for other's opinion as shown in Fig.3.

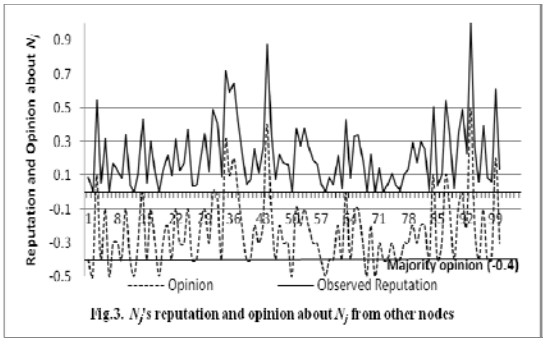
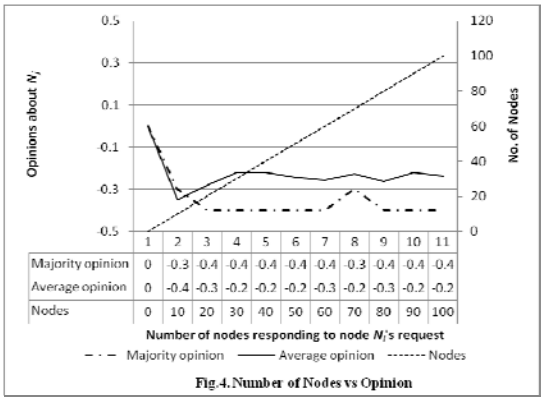


Fig.3. N_j's reputation and opinion about N_j from other nodes

The Fig.4 shows majority opinion when the number of responidng nodes for giving the opinon are varying. The average opinion, which will vary with the values given by responding nodes, is also shown. The majority opinion is almost constant except one, for sufficient number of transactions.



	1	2	3	4	5	6	7	8	9	10	11
Majority opinion	0	-0.3	-0.4	-0.4	-0.4	-0.4	-0.4	-0.3	-0.4	-0.4	-0.4
Average opinion	0	-0.4	-0.3	-0.2	-0.2	-0.2	-0.3	-0.2	-0.3	-0.2	-0.2
Nodes	0	10	20	30	40	50	60	70	80	90	100

Fig.4. Number of Nodes vs Opinion

In this paper, we presented a procedure to evaluate opinion values. These values are used to establish trust and thereby to give authorization. But the behavior of nodes with bad intentions and colluding with other nodes to get good opinion are hindrance to the trust establishment.

DOI: 01.IJNS.01.03.187

VI. Conclusion and Future Directions

With the emergence of widespread use of sensors in an urban environment, the need for a proper trust management between the collaborative entities and the need of the privacy control with each collaborative entity is strongly felt. Privacy control at the source will enable willing and engaged participation of citizens to create urban infrastructure with reduced cost. This work considered the problem of establishing trust with neighbors in a sufficiently large residential community by collecting opinions from others. The data is shared by setting authorization levels to others depending on trust. Trust estimation under malicious behavior of nodes, collusion between nodes to get authorization is a problem. Taking risk factor into consideration along with trust to exchange data are the areas to be considered for further study to have a robust trust management for participatory sensor networks.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commn. Mag., vol. 40, August 2002, pp. 102-114.

[2] C. Chong, and S.P. Kumar, "Sensor networks: Evolution, opportunities, and challenges," Proceedings of the IEEE, vol.91, August 2003, pp. 1247-56.

[3] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," Proc. ACM Mobicom'99, 1999, pp. 263-270.

[4] H. Chan, and A. Perrig, "Security and privacy in sensor networks," IEEE Computer, vol. 36, October 2003, pp. 103-105.

[5] D. Cuff, M. Hansen, and J. Kang, "Urban sensing: Out of the woods," Communications of ACM, vol.51, March 2008, pp. 24-33.

[6] D. Wright, D. et al., "The illusion of security," Communications. of ACM, vol. 51, March 2008, pp. 56-63.

[7] K. Shilton, "Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection," Communications of ACM, vol. 52, November 2009, pp. 48-53.

[8] Google, "Google flu trends," 2010, http://www.google.org/flutrends (2nd August 2010).

[9] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "AnonySense: Privacy-aware people centric sensing," Proc. ACM MobiSys'08, 2008, pp.2 11-224.

[10] Cisco, "Cisco Connected Real Estate for healthcare: Changing how hospital real estate is developed, used, and managed," 2009, www.cisco.com/.../healthcare/08CS1312-HC_Conn_RealEst_20090208.pdf (2nd August 2010), 6 pages.

[11] P.D. Giang, L.X. Hung, R.A. Shaikh, Y. Zhung, S. Lee, Y.K. Lee, and H. Lee, "A trust based approach to control privacy exposure in ubiquitous computing environments," Proc. IEEE Int. Conf. on Pervasive Services, 2007, pp. 149-152.

[12] R.A. Shaik, H. Jameel, S. Lee, S. Rajput, and Y.J. Song, "Trust management problem in distributed wireless sensor networks," Proc. 12th IEEE Int. Conf. on Embedded and Real Time Computing and Applications, IEEE Computer Society, 2006, 4 pages.

[13] H. Chen, H. Wu, X. Cao, and C. Gao, "Trust propagation and aggregation in wireless sensor networks," Proc. Japan-China Joint Workshop on Frontier of Computer Science and Technology, IEEE Computer Society, 2007, 8 pages.

[14] A. Mitseva, M. Gerlach, and N.R. Prasad, "Privacy protection mechanisms for hybrid hierarchical wireless sensor networks," Proc. IEEE ISWCS 2007, pp. 332-336.

DOI: 01.IJNS.01.03.187